UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS

I	NITED	STA	TFS OI	FAM	FRIC	Δſ
\mathbf{c}	\mathbf{n}	σ	\mathbf{L}		11/1/1/	$\overline{}$

v.

HAOYANG YU,

Case No. 19-cr-10195-WGY

Defendant

GOVERNMENT'S RESPONSE TO DEFENDANT'S SUPPLEMENTAL MEMORANDUM IN SUPPORT OF MOTION TO DISMISS FOR ALLEGED UNCONSTITUTIONAL SELECTIVE ENFORCEMENT

The defendant's latest brief presents a misleading and inaccurate portrayal of the preliminary investigation of the defendant, the justifications for that investigation, and the eventual referral of this matter to the U.S. Attorney's Office. Having now filed four separate briefs regarding this issue and having received additional law enforcement materials from the government concerning the origin and bases of this investigation, the defendant has not met his substantial burden of demonstrating both discriminatory intent *and* discriminatory effect. The Court should deny the defendant's motion and his request for additional discovery.

Contrary to the defendant's incomplete recitation of the facts, an objective assessment of *all* the available evidence does not support the defendant's contention that he was improperly targeted due to his ethnicity. Instead, the evidence shows that investigators pursued the defendant and his company, Tricon, because they reasonably suspected—based on two separate industry tips, statements from ADI witnesses, and ample other evidence—that he stole trade secrets with military applications from ADI and that he and Tricon may have violated U.S. export laws.

Aside from its inaccuracies and omissions, the defendant's supplemental brief focuses largely on references to "China" and the "PRC" (the "People's Republic of China") in various law

enforcement reports generated in the case, arguing that they are somehow evidence that the defendant was targeted due to his ethnicity. Def. Supp. Mot. at 8, 12-13. Given that this matter was initiated by the FBI as an economic espionage investigation, however, references to China or the defendant's "nexus" to China are hardly unexpected. "Economic espionage" is defined by statute as the theft of trade secrets for the benefit of a "foreign government, foreign instrumentality, See 18 U.S.C. § 1831.¹ Reports generated in economic espionage or foreign agent." investigations, therefore, *must* identify the foreign country suspected of benefitting from the stolen trade secrets and the target's nexus to it. A description of the defendant's "nexus" to the PRC in this context provides no evidence of purposeful discrimination. To the contrary, considered together with what was known about the defendant's company, the defendant's suspected theft of technologies with military applications, and the Chinese government's well-documented efforts to illicitly acquire the same types of technologies, it supported the agents' suspicions of economic espionage involving China – a threat that one senior Department of Justice official recently described "stand[ing] apart" from other nation states. See https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-olsen-delivers-remarkscountering-nation-state-threats.

There is no basis for further discovery regarding the defendant's claim. As the government described in its December 13, 2022, letter to the defense, *see* Def. Supp. Mot. At Exhibit A, it has already searched the investigative files of the participating agencies for materials concerning the origins of and justifications for the investigation. These and other materials produced prior to trial describe in plain terms how and why the agents chose to investigate the defendant and Tricon.

¹ Trade secret theft that does *not* involve the benefit of a foreign government or instrumentality is prohibited under a different section, 18 U.S.C. § 1832, of which the defendant was ultimately convicted.

There is no evidence, direct or indirect, of discriminatory intent in those materials such that further discovery might be warranted. Having failed to meet his selective enforcement burden even with the additional discovery, the defendant's motion must be denied.

The Preliminary Investigation of the Defendant and Tricon

Many of the facts discovered and relied upon by investigators during the preliminary investigation are described in the government's earlier selective enforcement filings. *See* ECF Nos. 68, 94, 317. For ease of reference, however, the government has compiled these facts chronologically below.

For context, the preliminary investigation occurred between late December 2017, when the Department of Commerce (DOC) received the initial private citizen referral about Tricon, and late March 2018, when the matter was first referred to the U.S. Attorney's Office for further investigation by both DOC and the FBI. The word "preliminary" aptly describes this phase of the investigation. It was conducted primarily through open sources in response to unsolicited, private-citizen tips received by two different agencies, without the benefit of grand jury or search warrant authorities (because the U.S. Attorney's Office was not yet involved). As the law enforcement reports fairly establish, the initial inquiry endeavored to assess the veracity of the private citizen tips and, thus, determine whether additional investigation of the defendant and Tricon was warranted. As described in greater detail below and in the government's earlier filings, the evidence yielded during this initial phase raised significant concerns that unquestionably necessitated further investigation of the defendant and Tricon. That evidence included the following:

- December 19, 2017 – DOC received a tip from Custom MMIC regarding Tricon. See Exhibit 1. The tip contained two basic allegations. First, after describing Tricon as "fishy," Custom MMIC reported that, "None of us here know this person or this company and there is 100% no way that [Tricon] could have come up with this product

line in 6 months. It is not possible." Second, the tip reported that one of Tricon's products, the TM5054, appeared to be controlled for export under the Commerce Control List (CCL) under a particular section, 3A001.b.2.d, that cites regional stability, nuclear proliferation, and anti-terrorism concerns.

- December 19, 2017 January 2018 DOC Special Agent Benjamin Hickok was assigned to investigate the December 19th tip, particularly the allegation that Tricon might be violating export controls applicable to dual-use items (like MMICs). Among other things, Special Agent Hickok confirmed the tip's information, including Tricon's Massachusetts business registration (dated March 2017), Tricon's mailing address (a UPS Store in Lexington), Tricon's website, and Tricon's various MMIC product offerings. See Exhibit 2.
- January 2018 Special Agent Hickok obtained a formal commodity classification indicating that the CCL controls the TM5054, the Tricon product highlighted by Custom MMIC, for regional stability, nuclear proliferation, and anti-terrorism reasons. See Exhibit 3. Based on their performance specifications, Special Agent Hickok believed that several of Tricon's other products are also export-controlled, meaning they had similar military applications to the TM5054.
- January 2018 Special Agent Hickok learned that the defendant and Tricon had never applied for or received any export licenses from DOC.
- January 23, 2018 Defense Security Service (DSS)³ received a tip from a security officer at Company A⁴ regarding "Jack Tricon, co-founder of Tricon MMIC (TM), LLC." See Exhibit 4. Company A, a cleared defense contractor⁵, was concerned that Tricon might be using Company A's intellectual property without authorization. Specifically, Company A reported that Tricon's website included an image of a

² The defendant omits any mention of this aspect of the December 19th tip in his supplemental brief. Because theft of trade secrets is a standard component of economic espionage, however, this aspect of the tip is especially noteworthy. The government further notes that trial evidence conclusively proved the validity of the tip's assertion: No one, including the defendant, could have designed Tricon's product line in six months. It further proved that the defendant had stolen his entire product catalog from ADI.

³ After January 2018, DSS changed its name to the Defense Counterintelligence and Security Agency, or DCSA. For purposes of this and the government's other selective enforcement filings, DSS and DCSA are the same.

⁴ The government is not publicly identifying Company A.

⁵ The term "cleared defense contractor" is defined as "a private entity granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense." *See* 10 USC § 393(e)(1).

microchip that a company employee did not believe was in the "open literature." *Id.* Company A also reported that Tricon's data sheets looked "just like" data sheets from Company A's predecessor company. *Id.* Investigators later learned that the defendant formerly worked at for Company A's predecessor company, thus validating the tipster's concerns that the defendant had misappropriated Company A's intellectual property.

- "suspicious contact report" concerning Tricon and the defendant. See Exhibit 5. In addition to discussing the substance of the Company A tip and providing basic biographical information about the defendant and his wife, whom public records identified as Tricon's owner and founder, the report noted the following about the defendant's alma mater, Tsinghua University (TU), which is located in China: "TU actively supports numerous Chinese military programs and researches subjects of military interest, including the Chinese nuclear program, satellite and potential antisatellite work and missile- and radar-related research. Lastly, they have previously sought sensitive, dual-use or export-controlled materials and components from [cleared contractors]." Id.6
- February 2018 The Company A referral and corresponding "suspicious activity report" were routed from DSS to FBI and NCIS in Boston, along with a Company A PowerPoint presentation that highlighted their concerns about Tricon. See Exhibit 6. Among other things, Company A cited the following as suspicious:
 - o Tricon is "using a picture of a Company A standard product on their front page."
 - Yanzhi Chen is identified as "owning" Tricon but has no apparent experience in MMIC design.
 - o Tricon's business address is a UPS store in Lexington.
 - o Tricon's data sheets are "the same format" as Company A's datasheets.
 - The defendant worked at Company A for 11 years (2002-2014)
- March 2018 Special Agent Hickok spoke with representatives from the defendant's former employer, ADI. They reported that: (1) Tricon's TM5054 data sheet was an "exact replica" of an ADI part and data sheet; (2) ADI "had suspicion[s] that [the defendant] may have been stealing the Intellectual Property (IP) during the time he was employed" at ADI; and (3) the defendant stopped working at ADI in August 2017, indicating that there was significant overlap—roughly five months—between the defendant's founding of Tricon and the defendant's leaving ADI. See Exhibit 2.
- March 22, 2018 DOC's Boston Field Office opened a formal investigation "to reveal if Tricon is involved in illegal export / diversion of specific technology in violation of 50 U.S.C. 1701-1706 (International Emergency Economic Powers Act), 18 U.S.C. 554 (Smuggling), and other possible violations." *Id.* Special Agent Hickok referred the

⁶ The defendant attaches the DSS report to his supplemental brief as Exhibit B but omits the portion describing this intelligence information regarding Tsinghua University. The complete version of the report, therefore, is attached hereto as Exhibit 5.

matter to the U.S. Attorney's Office, which accepted it. *Id.* This step made additional investigative resources available.

March 23, 2018 – FBI Boston opened a companion "economic espionage" investigation involving the defendant, Tricon, and Chen, Tricon's founder of public record. See Def. Supp. Mot. at Exhibit F. The FBI report documenting the opening of the investigation cited nearly all the information compiled by Company A, Custom MMIC, DSS, and DOC up to that point regarding the defendant's suspected theft of trade secrets. This included the information obtained by Special Agent Hickok from ADI. Additionally, because the investigation centered on possible economic espionage, the report described what was then known about the defendant's ties to China, including his significant travel there and his education in engineering physics at Tsinghua University, which supports the Chinese military's anti-satellite, missile, and radar-related research and has previously sought sensitive dual-use technologies from U.S. cleared contractors. Id.

The Legal Framework

The defendant's selective enforcement burden is "difficult to meet." *United States v. Washington*, 869 F.3d 193, 214 (3d Cir. 2017). According to the court in *Washington*:

Substantive claims of selective prosecution and selective enforcement are generally evaluated under the same two-part test, which is derived from a line of seminal Supreme Court cases about the collision between equal protection principles and the criminal justice system. A defendant challenging a criminal prosecution at either the law enforcement or prosecution inflection points must provide "clear evidence" of discriminatory effect and discriminatory intent (the latter is sometimes referred to as "discriminatory purpose"). Meeting this standard generally requires evidence that similarly situated individuals of a difference race or classification were not prosecuted, arrested, or otherwise investigated.

*Id.*⁷ "Awareness of consequences is not the same as intent to discriminate. The kind of intent to be proved is that the government undertook a particular course of action at least in part because

⁷ Even assuming a less stringent standard applies to discovery requests in the selective enforcement context, *see Washington*, 869 F.3d at 214, no further discovery is warranted here. Where discovery is appropriate, it is "essential" that it "start with limited inquiries" and to "enlarge the probe only if evidence discovered in the initial phase justifies a wider discovery program." *United States v. Davis*, 793 F.3d 712, 723 (7th Cir. 2015). The government here has already scoured the investigative files of FBI, DOC, HSI and DCIS, and voluntarily produced "[a]ll written or recorded case agent communications – created or sent prior to the case's referral to the U.S. Attorney's Office – that concern or describe how Haoyang Yu and Tricon MMIC, LLC, were

of, not merely in spite of, its adverse effects upon an identifiable group." *United States v. Turner*, 104 F.3d 1180, 1184 (9th Cir.1997) (internal quotation marks omitted); *see also Wayte v. United States*, 470 U.S. 598, 610 (1985) (stating that "[d]iscriminatory purpose ... implies more than ... intent as awareness of consequences") (internal quotation marks omitted).

The Court's June 13, 2022, Order (ECF No. 284) states that "a claim of selective enforcement is not governed by Armstrong and may be established by a fair preponderance of the Respectfully, the government disagrees that a substantive claim of selective evidence." enforcement can be established by a fair preponderance. The Court's position appears to be based on the Seventh Circuit's decision in *United States v. Davis*, 793 F.3d 712 (7th Cir. 2015). The court's holding in *Davis*, however, did not alter the *Armstrong* standard with respect to substantive claims of selective enforcement; it merely held that the standard for discovery in the selective enforcement context is relaxed compared to claims of selective prosecution because law enforcement agents do not enjoy the same "presumption of constitutional behavior" as prosecutors. Davis, 869 F.3d at 720. The Seventh Circuit in Washington (which was decided after Davis) discusses the Davis holding in great depth and concludes as follows: "as tacitly acknowledged by the Seventh Circuit, courts contemplating motions for discovery on selective enforcement claims must still be guided by the spirit of Armstrong/Bass, which incorporates the demands placed on the underlying substantive claims: not just 'some evidence,' but the heightened 'clear evidence' standard." Washington, 869 F.3d at 220. Consistent with the court's decision in Washington, therefore, the Court should apply Armstrong's "clear evidence" standard to the defendant's substantive claim.

identified as targets of a criminal investigation." Because these materials do not support the defendant's selective enforcement claim, a "wider discovery program" is not warranted. *Id.*

Argument

I. There Is No Evidence of Discriminatory Intent

The defendant's claim of discriminatory intent goes something like this: the agents' suspicions of export violations, trade secret theft, and economic espionage were not supported by sufficient evidence, and therefore, only ethnic discrimination explains their investigation. Yet an objective assessment of the information known to investigators when they referred this matter to the U.S. Attorney's Office—and before the agents could avail themselves of grand jury or search warrant authorities—leads to one conclusion: the investigation was directed by strong evidence of possible criminal wrongdoing, not by the defendant's ethnicity. Between December 2017, when DOC received the first tip about Tricon, and March 2018, when this matter was first referred to the U.S. Attorney's Office, three separate sources—Custom MMIC, Company A, and ADI—independently told law enforcement, in substance, that they suspected the defendant and Tricon of stealing trade secrets with military applications, violating U.S. export laws, or both. This is extraordinary. Just one of these reports would have been enough to justify further inquiry. But three separate reports, all of which were generally consistent and each of which was made independent of the others, could not be ignored.

⁸ Citing a report from the U.S. Naval Investigative Service (USNIS) from February 2018, *see* Def. Supp. Mot. at Ex. 8-9, the defendant erroneously states that agents continued to investigate him for export crimes despite "no apparent violation of the law." But this is simply not accurate. The USNIS report merely states that there was no specific evidence (based on Company A's tip) of "ITAR violations" by Tricon – that is, violations of the International Traffic in Arms Regulations, which govern the export of arms, munitions, and other similar items that fall under the U.S. Munitions List (USML). But considering that MMICs are not controlled under the USML, this notation in the USNIS report makes perfect sense. As described in contemporaneous reports, however, including those from DOC Special Agent Hickok, there was ample reason to believe that the defendant and Tricon may have committed export violations involving dual-use items (namely MMICs) under a different regulatory scheme: the Commerce Control List. And, of course, there was also a legitimate basis to conclude that the defendant may have committed other crimes, specifically, theft of trade secrets and economic espionage.

The defendant attempts to downplay the importance of these early tips by suggesting that neither the Custom MMIC report nor the Company A report "were among the allegations that the prosecution brought to trial." Def. Supp. Mot. at 6. There are two problems with this argument. *First*, it is blatantly false. Custom MMIC described Tricon as "fishy" and told DOC that "there is 100% no way that [Tricon] could have come up with this product line in 6 months. It is not possible." Company A similarly disputed the origin of Tricon's products, questioning whether the defendant stole the designs or was reselling another company's parts (possibly Company A's) under Tricon's name. In other words, in substance, both tips expressed concerns about Tricon's possible theft of trade secrets. Considering that a significant portion of the government's case-inchief proved the defendant's substantial theft of MMIC designs, the Custom MMIC and Company A reports went to the very heart of the government's case. Especially when combined with ADI's March 2018 report to Special Agent Hickok that ADI suspected the defendant of stealing trade secrets during his employment, the indications of trade secret theft suggested by these reports were striking and deserving of additional investigation.

Second, the defendant is wrong to suggest that the trial evidence is an appropriate measure of whether the agents' initial suspicions about the defendant and Tricon were untethered from his ethnicity. It is not reasonably in dispute that, in general, initial law enforcement suspicions are sometimes disproven by further investigation. Indeed, the entire purpose of opening a formal investigation is to determine whether suspicions are supported – or not – by evidence beyond a reasonable doubt. Even when investigations result in criminal charges, it is not uncommon for the allegations pursued at trial to differ, in big ways and small, from the agents' initial suspicions, particularly in long-term, complex investigations like this one. The fact that an initial allegation may not ultimately be borne out by evidence beyond a reasonable doubt, however, does not mean

the allegation was necessarily the product of improper motive. The only way to discern motive is to examine the agents' conduct during the investigation. Here, that conduct reflects no evidence of discriminatory intent.

Wholly apart from the significant evidence generated during the preliminary investigation, the defendant asks the Court to "infer" the agents' intent based on innocuous language in their reports. For example, the defendant cites to a U.S. Naval Investigative Service report from February 2018 that describes a "Red Dart" meeting in Dallas attended by various law enforcement and intelligence agencies. Def. Supp. Mot. at 8-9. He questions whether "Red Dart" is a code for "Red" China. Id. A simple Google search, however, reveals that "Red Dart" is an ordinary counterintelligence awareness program dating back to 2012 designed to enable industry to identify and prevent "industrial espionage and theft of intellectual property." See Exhibit 7. Similarly, the defendant attempts to "infer" discriminatory intent from references to "China" and the "PRC" in the agents' reports, namely the January 2018 DSS report (describing the Company A tip) and the March 2018 FBI report (opening an economic espionage investigation). Def. Sup. Mot. at 8, 12-13. However, a nexus to a "foreign government, foreign instrumentality, or foreign agent" is a fundamental element of all economic espionage investigations. See pp. 2-3, supra (citing 18 U.S.C. § 1831). By the very nature of the crime, the reports generated in these investigations must explore and describe the target's nexus to whatever foreign regime is at issue. The various descriptions of the defendant's nexus to China in law enforcement reports, therefore, are not circumstantial evidence of anything improper. They merely reflect the statutory reality of economic espionage.9

⁹ It bears noting that, almost universally, the references to China in the reports generated prior to the referral of this matter to the U.S. Attorney's Office focus on the defendant's *nexus* to China, not his ethnicity. In fact, the defendant's ethnicity is never mentioned in the reports, and

The initiation of an economic espionage investigation here was hardly the "inferential leap" that the defendant claims. Def. Supp. Mot. at 8, 12. By late March 2018, there were reasonable grounds to believe the defendant might have stolen trade secrets related to dual-use technologies and that the defendant had long-standing ties to China. These ties were hardly "illusory" as the defense claims. The defendant had spent considerable time in China and continued to travel there frequently, including just prior to his resignation from ADI. Moreover, the defendant received an engineering physics degree in China at a university that supports Chinese military programs and conducts engineering research in related subjects, including satellites, missiles, and radar. That university also has a history of attempting to obtain sensitive, export-controlled components from cleared contractors. The fact that, at the time of the investigation, the defendant had just finished working at ADI – a cleared contractor – in a group that designed export-controlled chips for, among other things, satellites, missiles, and radar was noteworthy.

At the same time, the defendant's ties to China were not the centerpiece of the agents' suspicions: they were a fact among a collection of many other facts. When the agents viewed this collection of facts alongside the substantial, well-documented threat of economic espionage posed by the Chinese government, the whole picture became more concerning. Even post-China Initiative, the Department of Justice has said that that the Chinese government "stands apart" from other nation state threats. See https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-olsen-delivers-remarks-countering-nation-state-threats. The Director of the FBI

his place of birth is mentioned in just one pre-referral report, in a section listing standard biographical information, and directly above an entry describing him as a United States citizen. *See* Def. Supp. Mot. at Exhibit F (p.7). While the defendant's name alone may suggest to some that he is ethnically Chinese-American, it is reasonable to assume that the reports would expressly refer to his ethnicity – indeed, emphasize it – if the decision to investigate him were motivated by ethnic bias.

acknowledged recently (again, post-China Initiative) that threats from the Chinese government are "more brazen [and] more damaging than ever before." *Id.* Those threats include, most notably, "the use of espionage [and] theft of trade secrets" and a "concerted effort [by the Chinese government] to steal our most sensitive information" including "cutting-edge semiconductor technology." *Id.* In light of this threat, the defendant's suspected theft of semiconductor technology with clear military applications, the description of his company by competitors as "fishy," his routine travel to China, and the fact that his alma mater (Tsinghua University) was reported to have "sought sensitive, dual-use ... export-controlled materials and components," and the other facts cited by the agents combined to raise strong and legitimate suspicions of economic espionage. There is no evidence that these suspicions were based in whole or in part on the defendant's ethnicity.

To be clear, the investigation of the defendant was not the product of a formal law enforcement initiative. As the government has repeatedly said for almost three years now, the investigation of the defendant and Tricon predates the China Initiative by nearly a year. *See* ECF No. 68 at 16. Nonetheless, even if this case were the product of a law enforcement initiative focused on Chinese nation-state threats (like the China Initiative), that does not provide support for the defendant's claim of purposeful discrimination. There is nothing *per se* unconstitutional about law enforcement initiatives focused on particular nation state threats—be it sanctions

Numerous other public and private institutions have reached the same or similar conclusions about the Chinese government. Several of these are identified in the government's initial opposition to the defendant's motion to dismiss. *See* ECF No. 68 at 14.

evasion by Russian oligarchs¹¹, drug trafficking by Mexican cartels¹², election interference by the Russian government¹³, or economic espionage by Chinese nation-state actors—even if those enforcement efforts *might* have a disproportionate impact on an identifiable group. That is because, in order to establish a substantive claim of selective enforcement, a defendant must show by "clear evidence" that law enforcement sought to investigate "because of, *not merely in spite of*," its adverse effects on an identifiable group. *United States v. Turner*, 104 F.3d 1180, 1184 (9th Cir. 1997) (emphasis added); *see also* ECF No. 68 at 16. In other words, "[a]wareness of consequences is not the same as intent to discriminate." *Id.* Without "clear evidence" of purposeful discrimination—of which there is none here—a claim of selective enforcement fails. *See Washington*, 869 F.3d at 214. This alone requires the denial of the defendant's motion.

II. The Defendant Has Not Proffered Clear Evidence of Discriminatory Effect

The defendant offers no new evidence of discriminatory effect in his supplemental brief. In his prior filings, he has not identified a single similarly-situated actor of a different ethnicity – much less a "pool" of them – who could have been investigated but was not. *See* ECF No. 68 at 7-13 & ECF No. 94 at 2-19. For this and the other reasons stated in the government's prior filings,

¹¹ See Announcement of Task Force KleptoCapture, available at https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.

¹² See Announcement of DOJ efforts to combat Mexican drug cartels, available at https://www.justice.gov/opa/pr/fact-sheet-department-justice-efforts-combat-mexican-drug-cartels.

¹³ See Concord Management & Consulting LLC, 18-cr-32 (D.D.C., Oct. 16, 2018) (denying Russian corporation's claim of selective enforcement, finding that company was prosecuted "because of their involvement in the Russian government's efforts to interfere in the 2016 presidential election —not because of their Russian nationality.")

see id., the defendant has not met his burden of showing clear evidence of discriminatory effect.

His motion to dismiss should be denied.

Conclusion

The defendant has failed to meet his burden of establishing clear evidence of both discriminatory intent and discriminatory effect. The Court should deny his motion to dismiss and his request for additional discovery.

Respectfully submitted,

RACHAEL S. ROLLINS United States Attorney

By: /s/ Jason A. Casey

Jason A. Casey Amanda Beck

Assistant U.S. Attorneys

Dated: April 14, 2023

Certification of Service

I hereby certify that these documents filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants.

/s/ Jason A. Casey

Jason A. Casey

Assistant U.S. Attorney

14